Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended): A smart card, comprising:

a communication unit to communicate with the outside;

an information accumulating unit to accumulate data and a program; and

an arithmetic processing unit to perform information processing,

~~wherein:~~

wherein said information accumulating unit stores value data, a transfer key ~~used to update~~ that updates the value data, a transfer key identifier ~~used to judge~~ that judges whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key ~~used to update~~ that updates the transfer key, and an upper limit of the transfer key identifier that represents an upper limit of the transfer key identifier that can be stored by the smart card~~;~~,

wherein said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the update key on the basis of common-key cryptography~~;~~, and

wherein said arithmetic processing unit ~~then~~ updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography.

2. (currently amended): A smart card according to claim 1, ~~wherein said arithmetic processing unit comprises the steps of:~~

wherein if command data that requests transmission of card information is received, said arithmetic processing unit transmits~~transmitting~~ the transfer key identifier to the outside as response data~~;~~.

wherein if command data that requests update permission of the transfer key is received, said arithmetic processing unit generates~~generating~~ a first random number and transmitting the first random number to the outside as response data~~;~~.

wherein if the command data which requests to obtain the transfer key, and which stores a second random number, is received, said arithmetic processing unit transmits~~transmitting~~ first encrypted data, into which the second random number, the transfer key identifier, and the transfer key are encrypted by use of the update key on the basis of common-key cryptography, to the outside as response data~~;~~. and

wherein if command data which requests update of the transfer key, and which stores second encrypted data, is received, said arithmetic processing unit decrypts~~decrypting~~ the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, updates~~updating~~ a value of the transfer key identifier to a value of the second data, and updates~~updating~~ a value of the transfer key to a value of the third data.

3. (currently amended): A smart card, comprising:

a communication unit to communicate with the outside;

an information accumulating unit to accumulate data and a program; and

an arithmetic processing unit to perform information processing,

~~wherein:~~

wherein said information accumulating unit stores value data, a transfer key ~~used to update~~ that updates the value data, a transfer key identifier ~~used to judge~~ that judges whether the transfer key is newer or older in accordance with a value of the transfer key identifier, a first public key certificate including a first public key, which ~~is used to update~~ updates the transfer key, a secret key corresponding to the first public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card~~;~~,

wherein said arithmetic processing unit updates the transfer key identifier and the transfer key by performing encryption using the first public key certificate and the secret key on the basis of public-key cryptography~~;~~, and

wherein said arithmetic processing unit ~~then~~ updates the value data by performing encryption using the transfer key on the basis of common-key cryptography.

4. (currently amended): A smart card according to claim 3, ~~wherein:~~

~~said arithmetic processing unit comprises the steps of:~~

wherein if command data that requests transmission of card information is received, said arithmetic processing unit transmits~~transmitting~~ the transfer key identifier and the first public key certificate to the outside as response data~~;~~,

wherein if command data which requests update permission of the transfer key, and which stores a second public key certificate including a second public key, is received, said arithmetic processing unit generates~~generating~~ a first random number and transmitting the first random number to the outside as response data~~;~~.

wherein if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, said arithmetic processing unit first ~~creating~~ creates first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next ~~creating~~ creates first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly ~~transmitting~~ transmits the first encrypted data and the first digital signature data to the outside as response data~~;~~. and

wherein if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, said arithmetic processing unit first ~~checking~~ checks the second digital signature data by use of the second public key on the basis of public-key cryptography, next ~~decrypting~~ decrypts the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, ~~updating~~ updates a value of the transfer key identifier to a value of the first data, and ~~updating~~ updates a value of the transfer key to a value of the second data.

5. (currently amended): A smart card, comprising:

a communication unit to communicate with the outside;

an information accumulating unit to accumulate data and a program; and an arithmetic processing unit to perform information processing,

~~wherein:~~

wherein said information accumulating unit stores value data, a transfer key ~~used to update~~ that updates the value data, a transfer key identifier ~~used to judge~~ that judges whether the transfer key is newer or older in accordance with a value of the transfer key identifier, an update key ~~used to update~~ that updates the transfer key, an update key identifier ~~used to judge~~ that judges whether the update key is newer or older in accordance with a value of the update key identifier, a first public key certificate including a first public key, which ~~is used to update~~ updates the transfer key, a secret key corresponding to the first public key, and an upper limit of transfer key identifier that represents an upper limit of the transfer key identifier which can be stored by the smart card~~;~~,

wherein said arithmetic processing unit updates the transfer key by use of the update key on the basis of common-key cryptography, or updates the transfer key by use of the first public key certificate and the secret key on the basis of common-key cryptography~~;~~, and

wherein said arithmetic processing unit ~~then~~ updates the value data by performing encryption using the transfer key on the basis of the common-key cryptography.

6. (currently amended): A smart card according to claim 5, ~~wherein:~~

~~said arithmetic processing unit comprises the steps of:~~

wherein if command data that requests transmission of card information is received, said arithmetic processing unit transmits~~transmitting~~ the transfer key identifier, the update key identifier, and the first public key certificate to the outside as response data~~;~~.

wherein if command data that requests update permission of the transfer key is received, said arithmetic processing unit generates~~generating~~ a first random number and ~~transmitting~~ transmits the first random number to the outside as response data~~;~~.

wherein if the command data which requests to obtain the transfer key, and which stores a second random number, is received, said arithmetic processing unit transmits ~~transmitting~~ first encrypted data, into which the second random number, the transfer key identifier, and the transfer key are encrypted by use of the update key on the basis of common-key cryptography, to outside as response data~~;~~. and

wherein if command data which requests update of the transfer key, and which stores second encrypted data, is received, said arithmetic processing unit first ~~decrypting~~ decrypts the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data, and third data, and next if the first data is equivalent to the first random number, and if a value of the second data is between a value of the upper limit of transfer key identifier and a value of the transfer key, ~~updating~~ updates a value of the transfer key identifier to a value of the second data, and ~~updating~~ updates a value of the transfer key to a value of the third data.

7. (currently amended): A smart card according to claim 5, ~~wherein:~~

~~said arithmetic processing unit comprises the steps of:~~

wherein if command data that requests transmission of card information is received, said arithmetic processing unit transmits~~transmitting~~ the transfer key identifier, the update key identifier, and the first public key certificate to the outside as response data~~;~~,

wherein if command data which requests update permission of the transfer key, and which stores a second public key certificate including a second public key, is received, said arithmetic processing unit generates~~generating~~ a first random number and transmitting the first random number to the outside as response data~~;~~,

wherein if command data which requests to obtain the transfer key, and which stores a second random number and a third public key certificate including a third public key, is received, said arithmetic processing unit first ~~creating~~ creates first encrypted data into which the transfer key identifier and the transfer key are encrypted by use of the third public key on the basis of public-key cryptography, next ~~creating~~ creates first digital signature data from the first encrypted data and the second random number by use of the secret key on the basis of public-key cryptography, and lastly ~~transmitting~~ transmits the first encrypted data and the first digital signature data to outside as response data~~;~~, and

wherein if command data which requests update of the transfer key, and which stores second encrypted data and second digital signature data, is received, said arithmetic processing unit first ~~checking~~ checks the second digital signature data by use of the second public key on the basis of public-key cryptography, next ~~decrypting~~ decrypts the second encrypted data by use of the secret key on the basis of public-key cryptography to extract first data and second data, and lastly if a value of the first data is between a value of the upper limit of transfer key identifier and a value of the transfer key, ~~updating~~ updates a value of the transfer key identifier to a value of the first data, and ~~updating~~ updates a value of the transfer key to a value of the second data.

8. (currently amended): A smart card, comprising:

a communication unit to communicate with the outside;

an information accumulating unit to accumulate data and a program; and

an arithmetic processing unit to perform information processing,

~~wherein:~~

wherein said information accumulating unit stores value data, ~~one~~ two or more transfer keys ~~used to~~ that update the value data, a ~~selection~~ transfer key identifier that includes a selection transfer key identifier that identifies the transfer key currently selected, and that identifies ~~used to identify~~ said two or more ~~the~~ transfer keys~~key currently selected~~, and an update key used to update the transfer key~~;~~,

wherein if the value of the transfer key identifier, which is received by said communication unit, is newer than that of said selection transfer key identifier, and which is equivalent to either a value of said transfer key identifier stored by said information accumulating unit, said arithmetic processing unit updates ~~the~~said selection transfer key identifier to the transfer key identifier received by said communication unit by performing encryption using the update key on the basis of common-key cryptography~~;~~, and

wherein said arithmetic processing unit ~~then~~ updates the value data by performing encryption using the transfer key corresponding to the update transfer key identifier on the basis of common-key cryptography.

9. (currently amended): A smart card according to claim 8,~~ wherein:~~

~~said arithmetic processing unit comprises the steps of:~~

wherein if command data that requests transmission of card information is received, said arithmetic processing unit transmits~~transmitting the~~ said selection transfer key identifier to the outside as response data~~;~~,

wherein if command data that requests update permission of the transfer key is received, said arithmetic processing unit generates~~generating~~ a first random number and transmitting the first random number to the outside as response data~~;~~,

wherein if the command data which requests to obtain the transfer key, and which stores a second random number, is received, said arithmetic processing unit transmits~~transmitting~~ first encrypted data, into which ~~the~~ said second random number, ~~the~~ said selection transfer key identifier~~, and the transfer key~~ are encrypted by use of ~~the~~ said update key on the basis of common-key cryptography, to the outside as response data~~;~~, and

wherein if command data which requests update of the transfer key, and which stores second encrypted data, is received, said arithmetic processing unit decrypts~~decrypting~~ the second encrypted data by use of the update key on the basis of common-key cryptography to extract first data, second data~~, and third data~~, and if the first data is equivalent to the first random number, and if a value of the second data which is equivalent to one of values of ~~the~~ said transfer key identifiers, and which is newer than that of said selection transfer key identifier used to identify said transfer key currently selected, ~~updating~~ updates a value of ~~the~~ said selection transfer key identifier to a value of the second data.

10.-19. (canceled)